Stream cipher based on pseudo-random number generation using optical affine transformation

Toru Sasaki[a], Hiroyuki Togo[a], Jun Tanida[a] and Yoshiki Ichioka[b]

[a]Graduate School of Engineering, Osaka University, 2 - 1 Yamadaoka,
Suita, Osaka 565-0871, Japan
[b]NARA National College of Technology, 22 Yatamachi, Yamatokoriyama,
Nara 639-1080, Japan

ABSTRACT

We propose a new stream cipher technique for 2-D image data which can be implemented by iterative optical transformation. The stream cipher uses a pseudo-random number generator (PRNG) to generate pseudo-random bit sequence. The proposed method for the PRNG is composed of iterative operation of 2-D affine transformation achieved by optical components, and modulo-n addition of the transformed images. The method is expected to be executed efficiently by optical parallel processing. We verify performance of the proposed method in terms of security strength and clarify problems on optical implementation by the optical fractal synthesizer.

Keywords: pseudo-random number, stream cipher, fractal, parallel processing

1. INTRODUCTION

In recent years, various types of information from a simple message in an e-mail system to a personal identification code in electronic commerce are running over communication networks. Information leakage is a serious problem in such networks, and data encryption is considered as a key technique against the problem. As characteristics of current web technology, massive image data are frequently dealt with on the Internet. For such large amount of contents, large keys are required to guarantee a high level of security, which requires us long computational time for encryption and decryption.

Optical computing techniques are expected to be useful for encryption of massive information because of parallel optical processing.[1-10] Encryption using encoding masks with random phase distributions has been proposed.[2] This method utilizes two statistically independent phase masks at the input and the Fourier planes and the target message is encrypted into stationary white noise. By experimental demonstration, performance of the method has been studied.[3,4] As the application of the technique, an encrypted memory has been studied.[5-7] A method using a stream cipher technique has been also proposed.[8-10] In this method, XOR operations between a random bit sequence and the message are executed in parallel by optical techniques. The random bit sequence, which is used as a key for encryption, is generated by a pseudo-random number generator (PRNG). To generate a random bit sequence, optical parallel processing can be applied effectively.

In this paper, we propose a new method of pseudo-random number generation, which is based on an optical feedback operation with 2-D affine transformations. Affine transformation is a kind of linear transformation composed of rotation, scaling, and translation. This transformation can be implemented in parallel by optical components. For example, a series of imaging lens, dove prism, and deflection mirror achieve it efficiently. Although the proposed method also requires modulo-n addition of images, this operation is expected to be achieved in parallel by a spatial light modulator. With small number of parameters, such as the rotation angle and the scaling factor, we can generate pseudo-random intensity distribution on a 2-D image. We verify the performance of the proposed method in terms of security strength by computer simulations and evaluate randomness of the patterns generated by the proposed PRNG. Finally, the proposed PRNG is implemented by the optical fractal synthesizer[11] to clarify problems in optical implementation of this method.

Further author information (Send correspondence to T. Sasaki)
T. S.: E-mail: sasaki@gauss.ap.eng.osaka-u.ac.jp
J. T.: E-mail: tanida@mls.eng.osaka-u.ac.jp

In *Optical Storage and Optical Information Processing*, Han-Ping D. Shieh, Tom D. Milster, Editors, Proceedings of SPIE Vol. 4081 (2000) • 0277-786X/00/$15.00

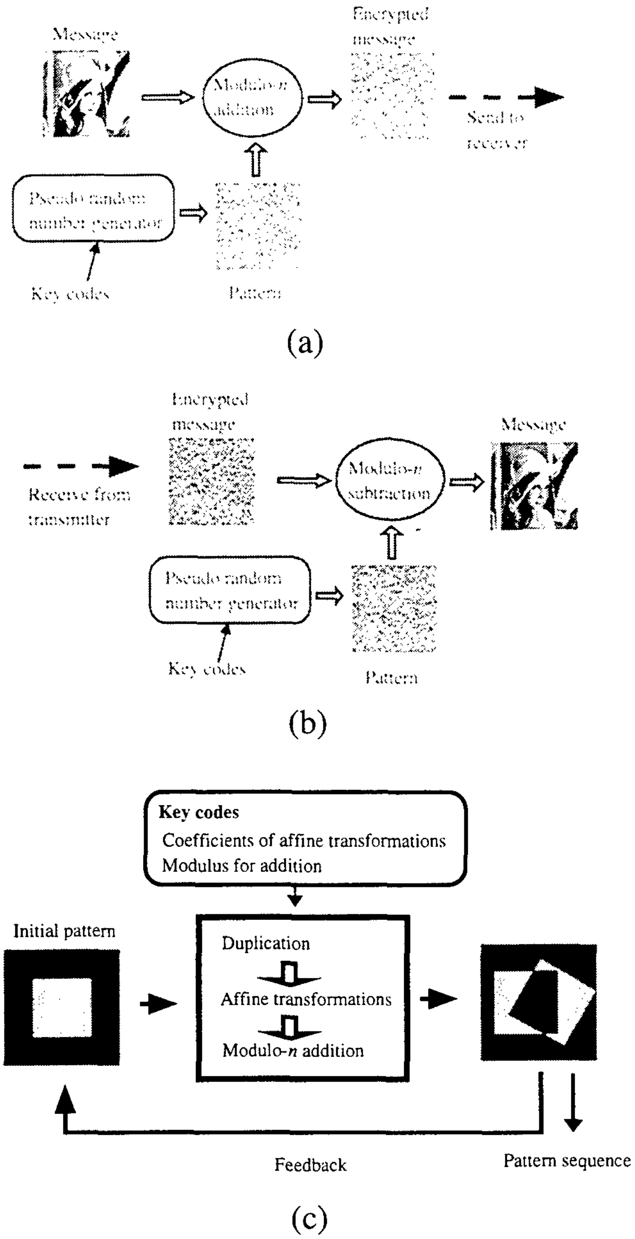


Figure 1. Schematic diagram of the proposed method: (a) encoding and (b) decoding methods, and (c) PRNG.

2. STREAM CIPHER USING 2-D AFFINE TRANSFORMATION

Figures 1 (a) and (b) show the schematic diagrams of encryption and decryption based on the stream cipher. In these diagrams, messages and patterns are 2-D images whose intensity is represented by 256 levels. Although 1-D bit sequences are often employed in the stream cipher, we use 2-D bit sequences on an image due to suitability for optical implementation. In the encryption, a message and a key pattern generated by the PRNG for a set of key codes are added in modulo-n. The encrypted message has random intensity distribution, which does not show any structure of the original message. In the decryption, the message is retrieved by subtracting the key pattern from the encrypted message in modulo-n. The key pattern is generated by the PRNG using the same key codes as the encoding ones.

Figure 1 (c) shows the schematic diagram of the proposed PRNG. This method is composed of affine transformations and feedback operations. Affine transformation is expressed by a set of a deformation matrix and a translation vector as follows:

$$\mathbf{x}' = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mathbf{x} + \begin{pmatrix} e \\ f \end{pmatrix}, \tag{1}$$

where $\mathbf{x}$ and $\mathbf{x}'$ are 2-D vectors representing the points on the input and the output planes. Several number of affine transformations are used for the PRNG. The initial image is multiplicated, and each image is transformed by any one of the affine transformations. The transformed images are summed up by addition in modulo-n. The resultant image is used as the input of the next step to generate another 2-D bit sequence.

The matrix in Eq. (1) can be rewritten for optical implementation. 2-D rotation and scaling implemented by a dove prism and a lens system are written by the following equations.

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \tag{2}$$

$$S(s) = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}, \tag{3}$$

where θ is the rotation angle and s is the scaling factor. In this paper, we use a specific affine transformation for the proposed PRNG represented by Eq. (4).

$$\mathbf{x}' = S(s)R(\theta)\mathbf{x} + \mathbf{t}, \tag{4}$$

where $\mathbf{t}$ is the translation vector representing image shift.

In this method, the key codes are assigned by the parameters of the affine transformations and the number of iterations. Space of the decoding key codes, which is expected to be large for high security strength, is determined by the possible combinatorial number of the parameters and the iteration. Although the space seems to be smaller than other implementations of the PRNG, high sensitivity on the parameter of the affine transformations enables us to increase available values for the parameter. Even if the number is insufficient, switching of several sets of affine transforms during iterations can be utilized to enlarge the key code space.

Figure 2 shows a sequence of 256 × 256 images generated by the PRNG with modulo 256 addition. A_i indicates the pattern generated by i times iteration. After 14 iterations, images with random intensity distribution are obtained.

Figures 3 (a) – (c) show the patterns generated by different parameter sets of the affine transformations and iterations. The parameter sets are shown in Table 1, where i is the identifier of affine transformation. Figures 3 (d) and (e) show the absolute value of intensity difference between Figs. 3 (a) and (b), and between (a) and (c), respectively. As seen from Figs. 3 (d) and (e), it is clear that these three patterns have different intensity distribution. Figure 3 (f) shows a specific case that random intensity distribution is localized into a fractal area. To use the proposed method for the stream cipher, the affine transformations and the iteration number must be selected to obtain a pattern where intensity is distributed randomly on the whole image. In this paper, to select the iteration number and the affine transformations, we calculate the autocorrelation function of the pattern, and verify if the autocorrelation function has only one peak on center of a plane like a delta function as described in the following section.

3. COMPUTER SIMULATION

To verify the effectiveness of the proposed method, we executed a computer simulation of data encryption and decryption. The message (the target image of cipher) is a 256 × 256 pixel image whose intensity is represented by 256 levels. Modulus for the image addition is 256. Figure 4 indicates (a) the message, (b) the key pattern, (c) the ciphered message, and (d) the decoded image. The key pattern is the same as the pattern in Fig. 3 (a). The ciphered message in Fig. 4 (c) has a pseudo-random intensity distribution in which the message content is not visible.

To verify security strength of the proposed method, we try to retrieve the message by slightly different key patterns. The key pattern is generated by the affine transformations whose parameters are modified from that of the encoding key. The encoding key pattern is the pattern in Fig. 4 (b). Table 2 indicates the modified parameters. Figures 4 (e), (f), and (g) show the decoded images by the key patterns with different scaling factor, rotation angle, and translation vector. The correct image can not be retrieved by these keys. Figure 4 (h) shows the decoded image

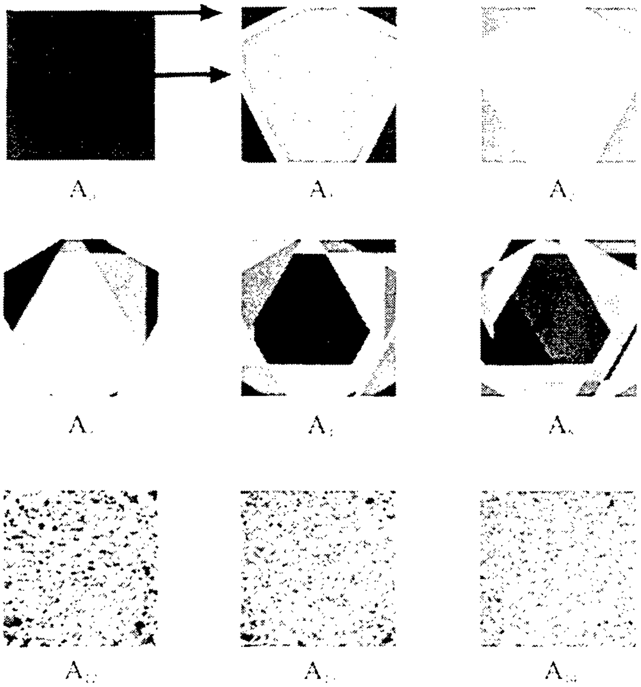


Figure 2. Image sequence generated by the PRNG.

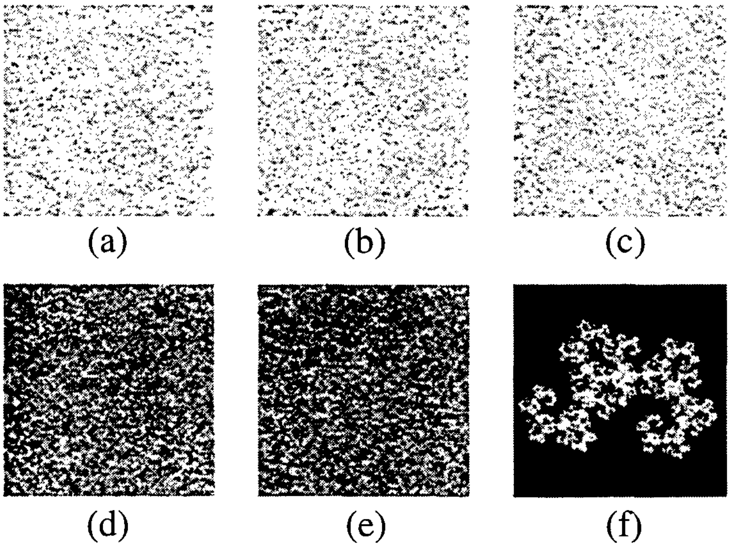


Figure 3. Patterns generated by different parameter sets of affine transformations.

Table 1. Coefficients of affine transformations for patterns of Figs. 3 (a), (b), (c), and (f).

Pattern	i	s_i	θ_i	$\mathbf{t}_i$	iteration
(a)	1	1.2	60	$(50,0)$	19
	2	1.2	120	$(-50,0)$	19
(b)	1	1.2	60	$(50,0)$	18
	2	1.2	120	$(-50,0)$	18
(c)	1	1.201	60	$(50,0)$	19
	2	1.201	120	$(-50,0)$	19
(f)	1	0.7	60	$(50,0)$	19
	2	0.7	120	$(-50,0)$	19

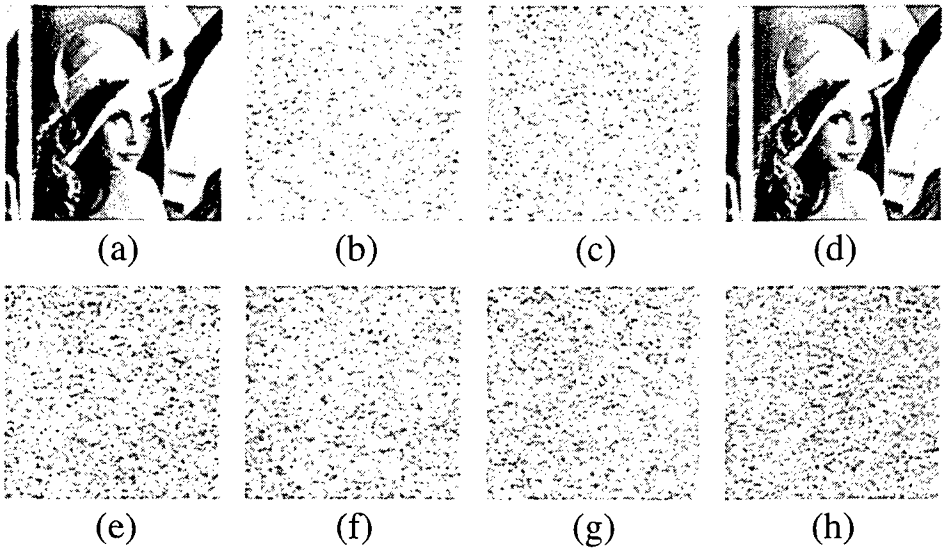
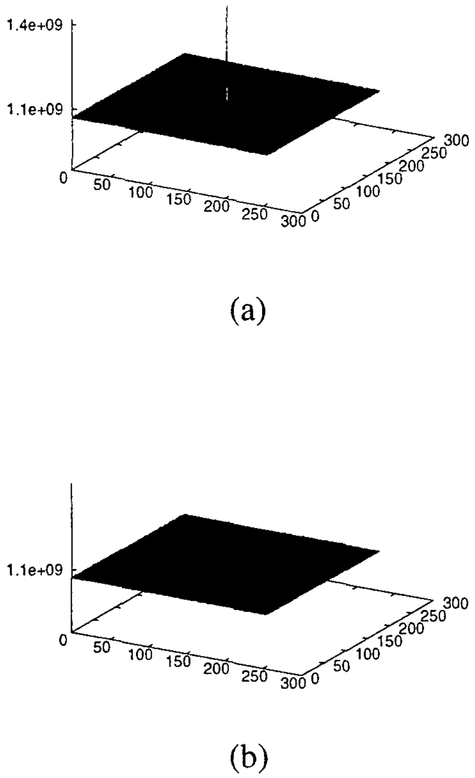


Figure 4. Verification of the proposed method: (a) message, (b) key pattern, (c) crypted message, and (d) encoded message. (e) – (h) are decoded image by slightly different key pattern, which are corresponding to Table 2.

Table 2. Modified parameters and variations.

Example	parameter	variation
(e)	s_1	+0.01
(f)	θ_1	+0.1
(g)	$\mathbf{t}_1$	$+(1,0)$
(h)	iteration	+1



(a)

(b)

Figure 5. Autocorrelation function of the generated patterns.

by the key pattern with the iteration number one time larger than that of the encoding key. Even in this case, the correct message can not be obtained. As seen from these results, it is very difficult to decrypt the message by the keys similar to the encoding ones.

Randomness of the intensity distribution is evaluated by statistical methods. In the case of a pattern with random intensity distribution, its autocorrelation function should be a delta function. Figure 5 (a) shows the autocorrelation function of the key pattern in Fig. 4 (b). It can be found that the autocorrelation function has only one peak on the center of pattern. As a consequence, the pattern is considered to have random intensity distribution.

It is expected that the patterns generated by different numbers of iterations has no correlation peak because they have different random distribution. Figure 5 (b) shows the correlation function between the patterns obtained by 18 and 19 iterations whose affine transformations are the same as in Fig. 4 (b). There is no peak on the correlation function. Therefore, we can verify that the patterns generated by the different number of iteration, even if the difference is just one, have different random distribution.

4. OPTICAL IMPLEMENTATION

To clarify problems on optical implementation of the proposed method, we constructed the PRNG on the optical fractal synthesizer.[11] Optical setup of the optical fractal synthesizer is shown in Fig. 6. This system can generate a fractal pattern for given system parameters by optical feedback processing. The input image of the optical fractal synthesizer is displayed on the CRT, and duplicated by the beam splitter BS1. Each image is rotated and reflected by the dove prism and translated by the tilted mirror in each optical path. The images passing through the different paths are combined by the second beam splitter BS2. After scaling by the zoom lens, the images are captured by

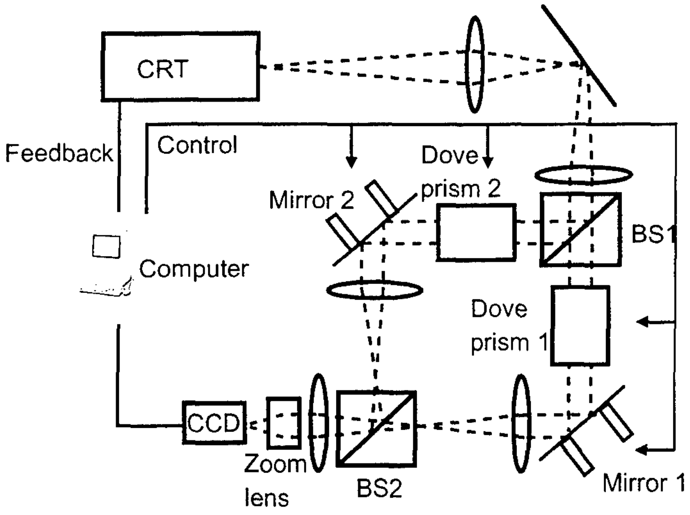


Figure 6. Optical setup of optical fractal synthesizer.

Table 3. Parameters of affine transformations used in optical implementation.

i	s_i	θ_i	$\mathbf{t}_i$
1	1.0	150	$(60, 0)$
2	1.0	30	$(-60, 0)$

the CCD camera. The captured image is displayed on the CRT again, and the same procedure is repeated. After a large number of iterations, the initial pattern is transformed into a complicated shape specified according to the system parameters.

To generate images with pseudo-random intensity distribution, the captured images through the different optical paths are added in modulo 2. XOR operation is used as modulo-2 addition, which is suitable for binary images. Figure 7 shows an example of pattern sequence generated by the optical system. Parameters of the affine transformation are shown in Table 3. The resolutional points of the image is 200 × 200 pixel. The overlapped area of two transformed patterns becomes dark by XOR operation executed by the computer. After 12 iterations, bright and dark pixels are spread over the image area.

Figures 8 (a)-(c) show results of message encryption and decryption using the optical PRNG, where the key pattern is the one obtained by 14 iterations shown in Fig. 7. In this case, the message is a binarized image to avoid effect of nonlinearity of the TV feedback system. As seen from Fig. 8 (c), the original message (Fig. 8 (a)) can not be retrieved. In addition, abstract structure of the message remains in the encrypted image of Fig. 8 (b). Difference between the key patterns independently generated by the same parameters is shown in Fig. 8 (d). As shown in this figure, the difference is relatively large. If we use the same key pattern as the encryption, the correct message is obtained as shown in Fig. 8 (e). It is clear that the obtained message is the same as the original.

We investigated the reason why the pattern can not be reproduced correctly. A histogram of an image captured by the CCD camera is shown in Fig. 9 (a), where the captured image is illustrated in Fig. 9 (b). The histogram has three peaks corresponding to the three areas (the black, dark, and white areas in Fig. 9 (b)). Note that there are many pixels whose intensity is between the peaks. To execute the XOR operation to the captured image, two threshold intensity values are set between the low and middle peaks, and between the middle and high peaks. We used 23 and 37 as the threshold values in this optical experiment. In the XOR operation, intensity values between the two threshold values are transformed to 255, the others are transformed to 0. In the case that intensity of the pixels on the CRT display fluctuates temporally, the pixels whose value is close to one of the threshold values become error sources.

Then we observed temporal transition of a pixel intensity in the captured image. In this experiment, a square

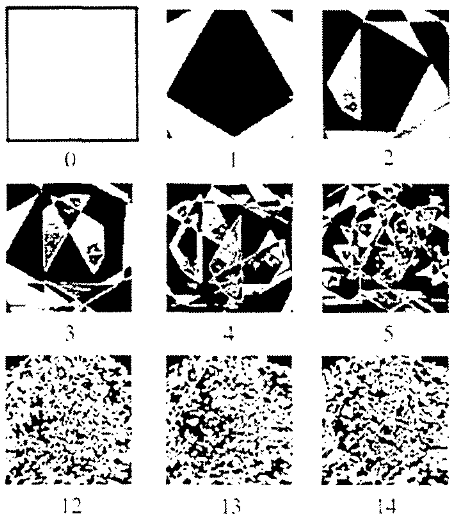


Figure 7. Random pattern sequence generated by the optical system.

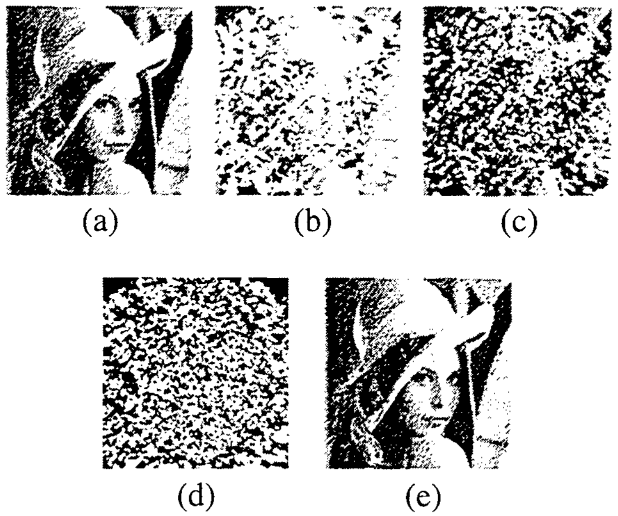


Figure 8. Result of optical implementation: (a) message, (b) data encrypted by a key generated optically, (c) message decoded by a key pattern generated independently, (d) intensity difference between the keys used for (b) and (c), and (e) message decoded by the key pattern used for (b).

pattern is displayed on the CRT at first step. Then the square pattern is transformed by the optical affine transformations shown in Table 3, and captured by the CCD camera. These processes are repeated 60 times. Finally, 60 images are obtained sequentially, and intensity transition of one pixel is measured from the images. Figure 10 shows the transition of the pixel whose location is (30, 200), where the coordinate system (x, y) is indicated in Fig. 9 (b). During the 60 iterations, intensity of the pixel fluctuates between 36 and 38 frequently. As seen from these results, reproduction of the same patterns is very difficult in this experimental system. To solve the problem, we should reduce the fluctuation of the pixel values, or reproduce the same fluctuation.

Slow speed of the optical feedback operation is also an important problem. In the experimental system, speed of feedback operation is limited by the transfer frame rate from the CCD camera to the CRT, which is about 30 frames per second. A high speed optical feedback system based on the smart pixels with parallel optical input/output ports and free-space optics is expected to overcome the problem.

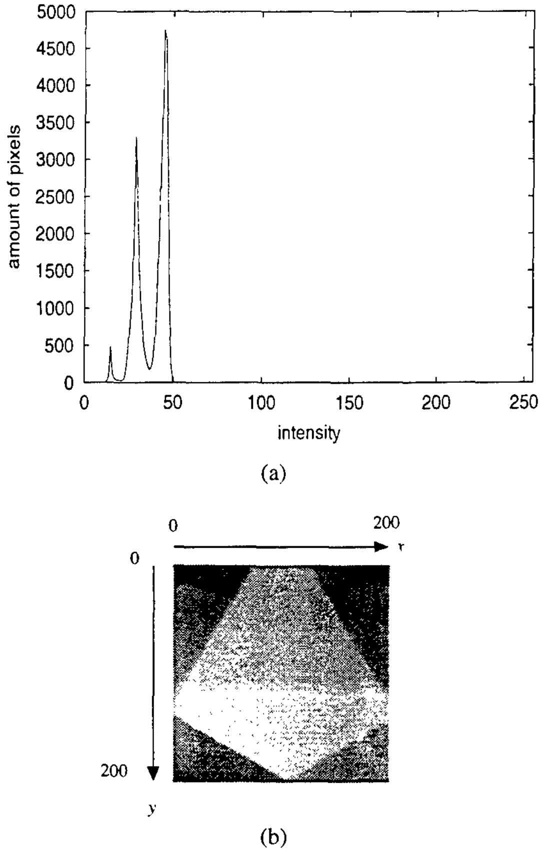


Figure 9. Histogram of an image captured by the CCD camera. (a) histogram and (b) captured image.

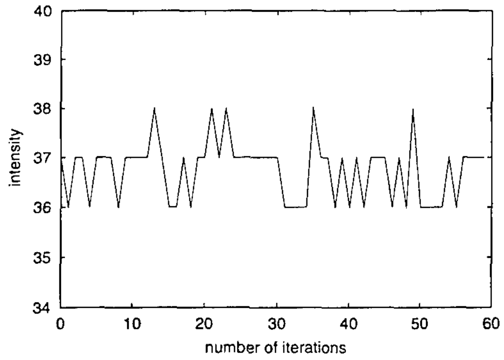


Figure 10. Temporal transition of pixel intensity.

5. CONCLUSION

We have proposed a method of stream cipher based on the PRNG using geometrical transformation, such as image rotation, scaling, and translations. The proposed method is suitable for optical implementation, and can generate 2-D pseudo-random intensity distribution by optical parallel affine transformations and optical feedback processing. Security strength of the method has been evaluated by computer simulations. It has been shown that different key pattern can not retrieve the ciphered image if sufficient number of iterations were done for random pattern generation. The proposed method was implemented on the optical fractal synthesizer, which suggests that uniformity of intensity distribution on the image plane is important for correct decoding.

REFERENCES

1. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.* **33**, pp. 1752–1756, 1994.
2. P. Refregier and B. Javidi, "Optical image encryption based on input plane and fourier plane random encoding," *Opt. Lett.* **20**, pp. 767–769, 1995.
3. B. Javidi, G. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," *Opt. Eng.* **35**, pp. 2506–2512, 1996.
4. B. Javidi, A. Sergent, and E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," *Opt. Eng.* **37**, pp. 565–569, 1998.
5. B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," *Appl. Opt.* **36**, pp. 1054–1058, 1997.
6. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," *Appl. Opt.* **37**, pp. 8181–8186, 1998.
7. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the fresnel domain," *Opt. Lett.* **24**, pp. 762–764, 1999.
8. M. Madjarova, M. Kakuta, M.Yamaguchi, and N. Ohyama, "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm," *Opt. Lett.* **22**, pp. 1624–1626, 1997.
9. M. Kakuta, M. Madjarova, T. Obi, M. Yamaguchi, and N. Ohyama, "Vernam encryption using optical parallel processing," *Jpn. J. Opt. (KOGAKU)* **27**, pp. 104–109, 1998.
10. S. Zhang and M. Karim, "High-security optical integrated stream ciphers," *Opt. Eng.* **38**, pp. 20–24, 1999.
11. J. Tanida, A. Uemoto, and Y. Ichioka, "Optical fractal synthesizer: concept and experimental verification," *Appl. Opt.* **32**, pp. 653–658, 1993.